S01P1068 US00

J1000 U.S. PTO
09/900584
07/06/01

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年 ７月１２日

出願番号
Application Number: 特願２０００－２１１７８７

出願人
Applicant(s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ５月２５日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００１－３０４４７１５

【書類名】　特許願
【整理番号】　0000629106
【提出日】　平成12年 7月12日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　中野　雄彦
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【先の出願に基づく優先権主張】
　【出願番号】　特願2000-205615
　【出願日】　平成12年 7月 6日
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9708842

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、並びに記録媒体

【特許請求の範囲】

【請求項１】　ネットワークを介して他の装置にコンテンツを送信する情報処理装置において、

前記コンテンツを暗号化する暗号化手段と、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証手段と、

前記認証手段の認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信手段と、

前記認証手段の認証結果に基づいて、前記他の装置の識別情報を取得する第１の取得手段と、

前記第１の取得手段により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する第１の計数手段と、

前記第１の計数手段により計数された前記識別情報を記憶する記憶手段と、

前記第１の計数手段により計数された前記受信台数の値に基づいて、前記認証手段の認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記認証手段の認証結果に基づいて、前記他の装置から受信台数の値を取得する第２の取得手段と、

前記第２の取得手段により取得された前記受信台数の値に基づいて、前記他の装置の受信台数を計数する第２の計数手段と

をさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記送信手段により前記他の装置に送信された前記解除鍵が変更された場合、前記記憶手段により記憶された前記識別情報を消去するとともに、前記計数手段により計数された前記受信台数の値をリセットする情報更新手段を

さらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　ネットワークを介して他の装置にコンテンツを送信する情報処理装置の情報処理方法において、

前記コンテンツを暗号化する暗号化ステップと、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信ステップと、

前記認証ステップの処理による認証結果に基づいて、前記他の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項５】　ネットワークを介して他の装置にコンテンツを送信する情報処理装置用のプログラムにおいて、

前記コンテンツを暗号化する暗号化ステップと、

前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、

前記認証ステップの処理による認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信ステップと、

前記認証ステップの処理での認証結果に基づいて、前記他の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶

制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項６】　第１のネットワークを介して第１の装置からコンテンツを受信する情報処理装置において、

前記第１の装置に対して、受信許可の要求を送信する第１の送信手段と、

前記第１の装置と認証する第１の認証手段と、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第１の装置から受信する受信手段と、

前記第１の装置から受信した前記コンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信手段と、

前記第２の装置より受信許可が要求された場合、前記第２の装置と認証する第２の認証手段と、

前記第２の認証手段の認証結果に基づいて、前記受信手段により受信された前記解除鍵を前記第２の装置に送信する第３の送信手段と、

前記第２の認証手段の認証結果に基づいて、前記第２の装置の識別情報を取得する第１の取得手段と、

前記第１の取得手段により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する第１の計数手段と、

前記第１の計数手段により計数された前記識別情報を記憶する記憶手段と、

前記第１の計数手段により計数された前記受信台数の値に基づいて、前記第２の認証手段の認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項７】　前記コンテンツを復号する復号手段と、

前記復号手段により復号された前記コンテンツを暗号化する暗号化手段と

をさらに備えることを特徴とする請求項６に記載の情報処理装置。

【請求項８】　前記第１の認証手段の認証結果に基づいて、前記第１の計数手段により計数された前記受信台数の値を、前記第１の装置に送信する第４の送信手段と、

前記第２の認証手段の認証結果に基づいて、前記第２の装置から受信台数の値を取得する第２の取得手段と、

前記第２の取得手段により取得された前記受信台数の値に基づいて、前記第２の装置の受信台数を計数する第２の計数手段と

をさらに備えることを特徴とする請求項６に記載の情報処理装置。

【請求項９】　前記第３の送信手段により前記第２の装置に送信された前記解除鍵が変更された場合、前記記憶手段により記憶された前記識別情報を消去するとともに、前記第１の計数手段により計数された前記受信台数の値をリセットする情報更新手段を

さらに備えることを特徴とする請求項６に記載の情報処理装置。

【請求項１０】　第１のネットワークを介して第１の装置からコンテンツを受信する情報処理装置の情報処理方法において、

前記第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、

前記第１の装置と認証する第１の認証ステップと、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第１の装置から受信する受信ステップと、

前記第１の装置から受信した前記コンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、

前記第２の装置より受信許可が要求された場合、前記第２の装置と認証する第２の認証ステップと、

前記第２の認証ステップの処理による認証結果に基づいて、前記受信ステップの処理により受信された前記解除鍵を前記第２の装置に送信する第３の送信ステップと、

前記第２の認証ステップの処理による認証結果に基づいて、前記第２の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記第２の認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項１１】　第１のネットワークを介して第１の装置からコンテンツを受信する情報処理装置用のプログラムにおいて、

前記第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、

前記第１の装置と認証する第１の認証ステップと、

前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第１の装置から受信する受信ステップと、

前記第１の装置から受信した前記コンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、

前記第２の装置より受信許可が要求された場合、前記第２の装置と認証する第２の認証ステップと、

前記第２の認証ステップの処理による認証結果に基づいて、前記受信ステップの処理により受信された前記解除鍵を前記第２の装置に送信する第３の送信ステップと、

前記第２の認証ステップの処理による認証結果に基づいて、前記第２の装置の識別情報を取得する取得ステップと、

前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、

前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、

前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記第２の認証ステップの処理での認証の成否を制御することにより、前記コンテン

ツの受信台数を制御する制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに記録媒体に関し、特に、コンテンツの利用を制限することができるようにした情報処理装置および方法、並びに記録媒体に関する。

【０００２】

【従来の技術】

近年、インターネットに代表されるネットワークシステムが普及してきた。これにより、ユーザは、インターネットを介して情報を発信したり、あるいは、情報を受け取ったりすることができる。

【０００３】

【発明が解決しようとする課題】

ところで、映画や音楽などの著作物の視聴を希望する利用者は、それに対する対価を支払うことにより、その著作物を受け取ることができる。

【０００４】

しかしながら、インターネットなどのネットワークを通じて、映画や音楽などの著作物が、その所有者だけでなく、著作物に対する対価を支払っていない多くの利用者に対して、不正に視聴されてしまう恐れがあった。

【０００５】

また、ネットワークを通じて不正に視聴される行為が無制限に行われるようになると、コンテンツ作成および流通ビジネスを阻害する恐れがあった。

【０００６】

本発明はこのような状況に鑑みてなされたものであり、コンテンツが、ネットワークを介して、不正に利用されるのを防止することができるようにするものである。

【０００７】

【課題を解決するための手段】

本発明の第１の情報処理装置は、コンテンツを暗号化する暗号化手段と、他の装置より受信許可が要求された場合、他の装置と認証する認証手段と、認証手段の認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信手段と、認証手段の認証結果に基づいて、他の装置の識別情報を取得する第１の取得手段と、第１の取得手段により取得された識別情報に基づいて、コンテンツの受信台数を計数する第１の計数手段と、第１の計数手段により計数された識別情報を記憶する記憶手段と、第１の計数手段により計数された受信台数の値に基づいて、認証手段の認証の成否を制御することにより、コンテンツの受信台数を制御する制御手段とを備えることを特徴とする。

【０００８】

本発明の第１の情報処理装置は、認証手段の認証結果に基づいて、他の装置から受信台数の値を取得する第２の取得手段と、第２の取得手段により取得された受信台数の値に基づいて、他の装置の受信台数を計数する第２の計数手段とをさらに設けるようにすることができる。

【０００９】

本発明の第１の情報処理装置は、送信手段により他の装置に送信された解除鍵が変更された場合、記憶手段により記憶された識別情報を消去するとともに、計数手段により計数された受信台数の値をリセットする情報更新手段をさらに設けるようにすることができる。

【００１０】

本発明の第１の情報処理方法は、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理での認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信ステップと、認証ステップの処理による認証結果に基づいて、他の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶

制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１１】

本発明の第１の記録媒体に記録されているプログラムは、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理での認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信ステップと、認証ステップの処理による認証結果に基づいて、他の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１２】

本発明の第１の情報処理装置、第１の情報処理方法、および第１の記録媒体に記録されているプログラムにおいては、コンテンツが暗号化され、他の装置より受信許可が要求された場合、その受信を許可しても受信台数が許容値を超えない限り、他の装置と認証され、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵が他の装置に送信される。

【００１３】

本発明の第２の情報処理装置は、第１の装置に対して、受信許可の要求を送信する第１の送信手段と、第１の装置と認証する第１の認証手段と、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第１の装置から受信する受信手段と、第１の装置から受信したコンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信手段と、第２の装置より受信許可が要求された場合、第２の装置と認証する第２の認証手段と、第２の認証手段の認証結果に基づいて、受信手段により受信された解除鍵を第２の装置に送信する第３の

送信手段と、第２の認証手段の認証結果に基づいて、第２の装置の識別情報を取得する第１の取得手段と、第１の取得手段により取得された識別情報に基づいて、コンテンツの受信台数を計数する第１の計数手段と、第１の計数手段により計数された識別情報を記憶する記憶手段と、第１の計数手段により計数された受信台数の値に基づいて、第２の認証手段の認証の成否を制御することにより、コンテンツの受信台数を制御する制御手段とを備えることを特徴とする。

【００１４】

本発明の第２の情報処理装置は、コンテンツを復号する復号手段と、復号手段により復号されたコンテンツを暗号化する暗号化手段とをさらに設けるようにすることができる。

【００１５】

本発明の第２の情報処理装置は、第１の認証手段の認証結果に基づいて、第１の計数手段により計数された受信台数の値を、第１の装置に送信する第４の送信手段と、第２の認証手段の認証結果に基づいて、第２の装置から受信台数の値を取得する第２の取得手段と、第２の取得手段により取得された受信台数の値に基づいて、第２の装置の受信台数を計数する第２の計数手段とをさらに設けるようにすることができる。

【００１６】

本発明の第２の情報処理装置は、第３の送信手段により第２の装置に送信された解除鍵が変更された場合、記憶手段により記憶された識別情報を消去するとともに、第１の計数手段により計数された受信台数の値をリセットする情報更新手段をさらに設けるようにすることができる。

【００１７】

本発明の第２の情報処理方法は、第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、第１の装置と認証する第１の認証ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第１の装置から受信する受信ステップと、第１の装置から受信したコンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、第２の装置より受信許可が要求された場合、第２の装置と認証する第２の認証ステップと、第

２の認証ステップの処理による認証結果に基づいて、受信ステップの処理により受信された解除鍵を第２の装置に送信する第３の送信ステップと、第２の認証ステップの処理による認証結果に基づいて、第２の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、第２の認証ステップの処理での認証の成否を制御することにより、コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１８】

本発明の第２の記録媒体に記録されているプログラムは、第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、第１の装置と認証する第１の認証ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第１の装置から受信する受信ステップと、第１の装置から受信したコンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、第２の装置より受信許可が要求された場合、第２の装置と認証する第２の認証ステップと、第２の認証ステップの処理による認証結果に基づいて、受信ステップの処理により受信された解除鍵を第２の装置に送信する第３の送信ステップと、第２の認証ステップの処理による認証結果に基づいて、第２の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、第２の認証ステップの処理での認証の成否を制御することにより、コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１９】

本発明の第２の情報処理装置、第２の情報処理方法、および第２の記録媒体に記録されているプログラムにおいては、第１の装置より第１のネットワークを介して受信したコンテンツが、第１の装置より得た許可台数を上限に、第２のネッ

トワークを介して第２の装置に送信される。

【００２０】

【発明の実施の形態】

図１は、本発明を適用したネットワークシステムの構成例を示すブロック図である。このネットワークシステムにおいては、ソース１が、バス４－１を介して、シンク２－１およびブリッジ３－１に接続され、また、ブリッジ３－１が、バス４－２を介して、シンク２－２およびブリッジ３－２に接続され、さらに、ブリッジ３－２が、バス４－３を介して、シンク２－３，２－４に接続されている。

【００２１】

ソース１は、コンテンツを出力する出力装置である。コンテンツを出力する場合、ソース１は、コンテンツを暗号化した後、バス４－１乃至４－３を介して、シンク２－１乃至２－４に出力する。なお、暗号化されたコンテンツの復号に必要な鍵情報は、認証処理に成功したシンクにだけ渡される。これにより、コンテンツを受信するシンクの台数が制限される。なお、後述するブリッジ３－１，３－２は、受信した信号を再出力するだけなので、台数カウントの対象から除外される。

【００２２】

シンク２－１乃至２－４（以下、シンク２－１乃至２－４を個々に区別する必要がない場合、単にシンク２と記載する。その他の装置においても同様とする）は、ソース１より供給されたコンテンツを受信する受信装置である。認証処理に成功した場合、シンク２は、ソース１より渡された鍵情報に基づいて、受信したコンテンツを復号する。ただし、ブリッジ３－１や３－２が暗号を一旦解き、新たな鍵で暗号化して出力する場合は、シンク２－２乃至２－４は直接つながるブリッジより渡された鍵情報に基づいて、受信したコンテンツを復号する。

【００２３】

ブリッジ３－１，３－２は、ソース１より出力された、暗号化されているコンテンツを受信し、復号した後、再び暗号化してシンク２－２乃至２－４に出力するものとする。そのため、ブリッジ３－１は、ソース１と認証処理を行い、暗号

化されたコンテンツの復号に必要な鍵情報を取得するとともに、再出力するコンテンツを何台のシンク２に受信させたいかをソース１に伝える。そして、ブリッジ３－１は、ソース１から許可を得たら、ソース１に代わって、コンテンツを受信するシンク２－２乃至２－４の台数を制限する。なお、ブリッジ３－２は、ブリッジ３－１と認証し、同様にシンク２－３，２－４の受信台数を制限する。

【００２４】

図２は、ソース１の詳細な構成例を示すブロック図である。

【００２５】

コンテンツプレーヤ１１は、メディア１２が装着されると、制御部１５の制御に基づいて、メディア１２に記録されているコンテンツを再生し、暗号部１３に出力する。暗号部１３は、コンテンツプレーヤ１１より入力されたコンテンツを暗号化し、通信I/F（インタフェース）１４を介して、外部に出力する。なお、コンテンツプレーヤ１１とメディア１２の代わりに、放送コンテンツを受信し、出力するチューナーを持つソースも考えられる。

【００２６】

制御部１５は、コンテンツプレーヤ１２、暗号部１３、通信I/F１４、および記憶部１６を制御する。制御部１５はまた、コンテンツプレーヤ１１で再生されたコンテンツを、必要に応じて、記憶部１６に記憶させる。

【００２７】

図３は、シンク２の詳細な構成例を示すブロック図である。

【００２８】

制御部２４は、画像・音声出力部２１、復号部２２、通信I/F２３、および、記憶部２５を制御する。制御部２４はまた、通信I/F２３を介して送信されてきた、暗号化されているコンテンツを復号部２２に送る。

【００２９】

復号部２２は、通信I/F２３を介してソース１より送信されてきた鍵情報を取得する。復号部２２はまた、コンテンツを、取得した鍵情報に基づいて復号する。画像・音声出力部２１は、復号部２２で復号されたコンテンツを出力する。

【００３０】

図４は、ブリッジ３の詳細な構成例を示すブロック図である。

【００３１】

制御部３５は、通信I/F３１、復号部３２、暗号部３３、通信I/F３４、および、記憶部３６を制御する。制御部３５はまた、通信I/F３１を介して送信されてきた、暗号化されているコンテンツを復号部３２に送る。

【００３２】

復号部３２は、通信I/F３１を介してソース１より送信されてきた鍵情報を取得するとともに、受信コンテンツを、取得した鍵情報に基づいて復号する。

【００３３】

暗号部３３は、復号部３２で復号されたコンテンツを暗号化し、通信I/F３４を介して、外部に出力する。

【００３４】

なお、認証には、公開鍵暗号技術を用いるものとし、ソース１、シンク２、およびブリッジ３は鍵管理組織が発行する各機器用のDigital Certificate（以下、Certificateと記載する）と各機器用の秘密鍵と鍵管理組織の公開鍵を持つものとする。このCertificateには各機器用の秘密鍵と対応する各機器用の公開鍵、その機器の固有ID、そしてこの２つのデータに対する鍵管理組織による電子署名が含まれるものとする。

【００３５】

図５は、ソース１とシンク２－１（図１）が、直接接続される場合の認証処理を説明する図である。

【００３６】

まず、シンク１が自分のCertificateをソース２－１に送信する。具体的には、シンク１の制御部１５が、記憶部１６からCertificateを読み出し、通信I/F１４を介して、ソース２－１に通信コマンドとして送信する（図５①）。

【００３７】

ソース２は、この通信コマンドを受信すると、そのデータが正当なものか否かを判定する。具体的には、ソース２－１の制御部２４が、記憶部２５に記憶されている鍵管理組織の公開鍵を用いて、通信I/F２３を介して受信したCertificate

中のデータと、それらに付随する鍵管理組織の電子署名が対応しているのか否かを調べる。すなわち、制御部２４は、公開鍵暗号のDSA（Digital Signature Algorithm）Verify演算処理を実行することにより、受信データの正当性を判定する。そして、判定結果が、正当である場合、認証処理を継続し、そうでない場合、認証処理を終了する。

【００３８】

処理を継続する場合、ソース１の制御部１５は、Certificate中の相手のIDが記憶部１６に保持する認証済みIDリスト（以下、IDリストと記載する）に登録済みであるか否かを調べ、登録済みの場合、変数CntUpに０を代入する。

【００３９】

一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース１の制御部１５は、受信を許可したシンク２の数（以下、変数SinkCntと記載する）と受信を許可できる上限数（以下、変数MaxSinkと記載する）を比較し、変数SinkCntの方が小さければ変数CntUpに１を代入する。

【００４０】

なお、SinkCnt＝MaxSinkの場合、認証処理は終了される。また、変数MaxSinkは、変数でなくてもよい（すなわち、定数であってもよい）。

【００４１】

そして、ソース１の制御部１５は、擬似乱数生成アルゴリズムにより、擬似乱数Random_challengeを生成し、シンク２に通信コマンドとして送信する（図５②）。

【００４２】

シンク２－１の制御部２４は、この通信コマンドを受信すると、その値に対して、記憶部２５に保持されている自分自身の秘密鍵を用いて、公開鍵暗号のDSASign演算処理を実行して、電子署名を計算する。シンク２－１の制御部２４は、計算された電子署名を、通信コマンド（Responseデータ）として、ソース１に送信する（図５③）。

【００４３】

ソース１の制御部１５は、この通信コマンドを受信すると、自分が送った擬似

乱数Random_challengeとこの電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当である場合、認証処理が継続され、そうでない場合、認証処理は終了される。

【００４４】

処理を継続する場合、ソース１の制御部１５は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク２－１に通信コマンドとして送信し（図５④）、変数SinkCntの値を変数CntUpの値だけ増加する。そして、ソース１の制御部１５は、Certificate中の相手のIDが記憶部１６に保持する認証済みIDリストに登録済みであるか否かを調べ、登録済みの場合、変数CntUpに０を代入する。一方、IDリストにCertificate中の相手のIDが未登録の場合、変数SinkCntと変数MaxSinkを比較し、変数SinkCntの方が小さければ変数CntUpに１を代入する。

【００４５】

シンク２－１は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことによって、コンテンツを受信することができる。

【００４６】

また、図１に示されるソース１とシンク２－２のように、ソース１より出力されたコンテンツが、ブリッジ３－１を経由した後に、シンク２－２に受信される場合、やはり、シンク２－２とブリッジ３－１は、図５に示されたような認証処理を行う。すなわち、ソース１とシンク２－３、または、ソース１とシンク２－４のように、２台以上のブリッジ経由でコンテンツが伝送される場合でも、シンク１と最後のブリッジ３－２（シンク２－３，２－４と直接つながるブリッジ）は同様の認証処理を行う。

【００４７】

以上の認証処理におけるシンク２の処理フローを図６に、ソース１の処理フローを図７に、それぞれ示す。

【００４８】

シンク１の認証処理は、相手がブリッジ３であっても、ソース２の場合と全く

同じである。ブリッジ３の認証処理は、図７のステップＳ１５に示す処理が、ソース２の場合と異なる。具体的には、SinkCnt＝MaxSinkの場合、ブリッジ３は、変数MaxSinkの値を大きくするために、自分自身が受信（入力）しているコンテンツの発信元であるソース１またはブリッジ３（図１の例の場合、ブリッジ３－１ならソース１、ブリッジ３－２ならブリッジ３－１）に受信許可を要求する認証処理を行う。なお、この場合には、１台以上の受信台数の追加が要求される。この認証処理が成功した場合、図７のステップＳ１６以降の処理が継続される。

【００４９】

図８は、ソース１とブリッジ３－１（図１）が、直接接続される場合の認証処理を説明する図である。

【００５０】

まず、ブリッジ３－１の制御部３５は、自分のCertificate、変数RelCntおよび変数AbsCntをソース１に送信する（図８①）。ここで、変数RelCntは、ブリッジ３－１が新たに得たい受信許可の台数を表わし、変数AbsCntは、既に得ている許可台数と今回許可を得たい台数の合計台数を表わしている。

【００５１】

ソース１の制御部１５は、これを受信すると、Certificateが正当なものか否かを、上述したDSA Verify演算処理を実行することにより判定する。そして、判定結果が、正当でない場合、認証処理は終了される。

【００５２】

処理を継続する場合、ソース１の制御部１５は、Certificate中の相手のIDが自分のIDリストに登録済みか否かを調べ、登録済みの場合、変数CntUpに変数RelCntを代入する。

【００５３】

一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース１の制御部１５は、変数CntUpに変数AbsCntを代入する。そして、ソース１の制御部１５は、変数SinkCntに変数CntUpを加えた値が、変数MaxSinkより小さいか否かを判定し、等しい場合、認証処理を終了する。

【００５４】

そして、ソース１の制御部１５は、擬似乱数Random_challengeを生成し、ブリッジ３－１に通信コマンドとして送信する（図８②）。

【００５５】

ブリッジ３－１の制御部３５は、この通信コマンドを受信すると、その値と送信済みの変数RelCntと変数AbsCntに対して、記憶部３６に保持されている自分自身の秘密鍵を用いて、上述したDSA Sign演算処理を実行して、電子署名を計算する。ブリッジ３－１の制御部３５は、計算された電子署名を、通信コマンド（Responseデータ）として、ソース１に送信する（図８③）。

【００５６】

ソース１の制御部１５は、この通信コマンドを受信すると、自分が送った擬似乱数Random_challenge、受信済みの変数RelCntおよび変数AbsCntに、この電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当でない場合、認証処理は終了される。

【００５７】

処理を継続する場合、ソース１の制御部１５は、コンテンツにかけた暗号を解くのに必要な鍵情報をブリッジ３－１に通信コマンドとして送信し（図８④）、変数SinkCntの値を変数CntUpの値だけ増加させた後、相手のIDがIDリストに未登録の場合、追加する。

【００５８】

ブリッジ３－１は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解いた後、再び暗号化してコンテンツを出力する。そして、ブリッジ３－１の制御部３５は、変数MaxSinkの値を変数RelCntの値だけ増加する。

【００５９】

以上の認証処理におけるブリッジ３の処理フローを図９に、またソース１の処理フローを図１０に、それぞれ示す。

【００６０】

また、図１に示されるソース１とシンク２－３、またはソース１とシンク２－

４のように、ソース１より出力されたコンテンツが、２台以上のブリッジ３－１，３－２を経由した後に、シンク２－３，２－４に受信される場合、やはり、コンテンツを出力するブリッジ３－１（以下、Txブリッジと記載する）とそれを受け取るブリッジ３－２（以下、Rxブリッジと記載する）は、図８に示されたような認証処理を行う。

【００６１】

なお、Rxブリッジの認証処理は、相手がソース１の場合と全く同じである。

【００６２】

Txブリッジの認証処理は、図１０のステップＳ４６に示す処理が、ソース１の場合と異なる。具体的には、SinkCnt＋CntUp＞MaxSinkの場合、Txブリッジは、変数MaxSinkの値を大きくするために、自分自身が入力しているコンテンツの発信元であるソース１またはブリッジ３に受信許可を要求する認証処理を行う（図１の例の場合、ブリッジ３－１はソース１に認証を要求する）。なお、この場合には（（SinkCnt＋CntUp)－MaxSink）以上の受信台数の追加が要求される。この認証処理が成功した場合、図１０のステップＳ５０以降の処理が継続される。

【００６３】

また、他の処理例としては、変数RelCntおよび変数AbsCntが、Certificateとは別に送信される場合が考えられる。例えば、図８③に示されたResponseと共に送信する方法、あるいは、全く別の通信コマンドで送信する方法もある。

【００６４】

また、図７のステップＳ１５、または、図１０のステップＳ４６において、ブリッジ３－１，３－２が、新たに接続されたソース１かブリッジ３と認証を行う場合、その結果によらず、その後の処理は継続しない方法もある。すなわち、新たな認証は、次回以降の認証を成功させるためのものと位置付けることができる。

【００６５】

さらにまた、シンク２が自分の出力を受けるのを止め、暗号を解くのに必要な情報を失った場合、ソース１またはブリッジ３は、変数SinkCntをそのシンク２の分だけ減らすことができる。例えば、ソース１やブリッジ３がコンテンツにか

ける暗号の鍵情報を変更したら、シンク２は、自分自身の変数SinkCntを０にすることができる。

【００６６】

以上のように、ソース１またはブリッジ３が、出力を受けられるシンク２の受信台数を制限するようにしたので、以下に示すような効果が得られる。

（１）コンテンツに関する権利者は、コンテンツの不正視聴や記録を未然に防ぐことができる。

（２）ブリッジを使って信号を再出力した場合でも、ソースは、ブリッジの先にいるシンクも含め、台数を制限することができる。

（３）台数の制限を機器固有のIDを使って行うことで、同じシンクが何度認証しても台数を誤って増やすことが無い。

（４）ブリッジが受信許可をソースや別のブリッジに要求する際に、受信台数の増加または減少分と受信合計台数を知らせることで、ソースや別のブリッジは、そのブリッジと認証したことがある場合、あるいは、認証したことがない場合のいずれにおいても、変数SinkCntを容易に、正しい値に変更することができる。

（５）公開鍵暗号技術を用いることで、機器固有IDや要求台数を、安全に他の機器に渡すことができ、かつ、正しい台数管理を行うことができる。

【００６７】

上述した一連の処理は、ハードウエアにより実行させることもできるが、ソフトウエアにより実行させることもできる。一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【００６８】

この記録媒体は、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD（Mini-Disk）を含む）、もしくは

半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMやハードディスクなどで構成される。

【００６９】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【００７０】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【００７１】

【発明の効果】

以上のように、本発明の第１情報処理装置、第１の情報処理方法、および第１の記録媒体に記録されているプログラムによれば、コンテンツを暗号化し、他の装置より受信許可が要求された場合、その受信を許可しても受信台数が許容値を超えない限り、他の装置と認証し、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信するようにしたので、コンテンツの利用を制限することが可能になる。

【００７２】

また、本発明の第２の情報処理装置、第２の情報処理方法、および第２の記録媒体に記録されているプログラムによれば、第１の装置より第１のネットワークを介して受信したコンテンツを、第１の装置より得た許可台数を上限に、第２のネットワークを介して第２の装置に送信するようにしたので、出力コンテンツの受信装置を、得た許可台数に基づいて制限することが可能になる。

【図面の簡単な説明】

【図１】

本発明を適用したネットワークシステムの構成例を示すブロック図である。

【図２】

図１のソースの詳細な構成例を示すブロック図である。

【図３】

図１のシンクの詳細な構成例を示すブロック図である。

【図４】

図１のブリッジの詳細な構成例を示すブロック図である。

【図５】

ソースまたはブリッジとシンクの認証処理を説明する図である。

【図６】

シンクのソースまたはブリッジに対する認証処理を説明するフローチャートである。

【図７】

ソースまたはブリッジのソースに対する認証処理を説明するフローチャートである。

【図８】

ソースまたはTxブリッジのRxブリッジの認証処理を説明する図である。

【図９】

Rxブリッジのソースまたは Txブリッジに対する認証処理を説明するフローチャートである。

【図１０】

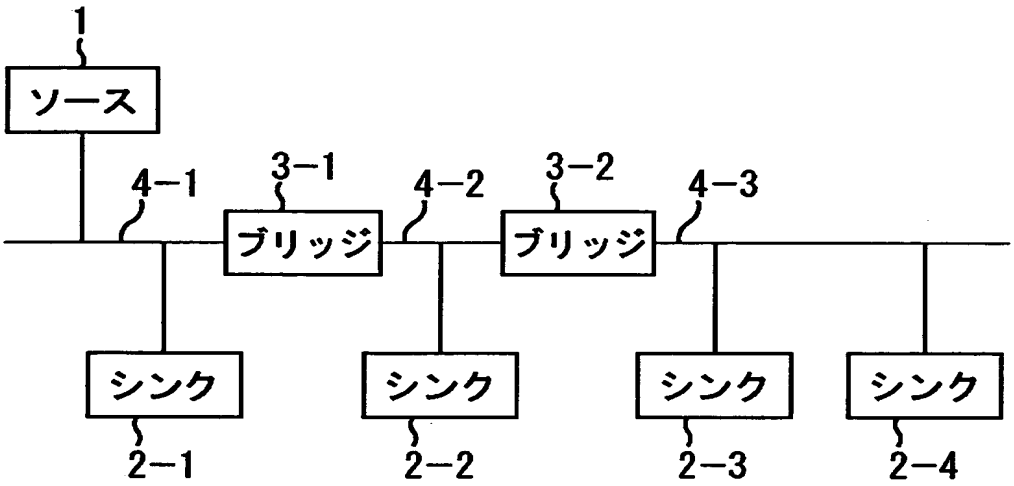
ソースまたはTxブリッジのRxブリッジに対する認証処理を説明するフローチャートである。

【符号の説明】

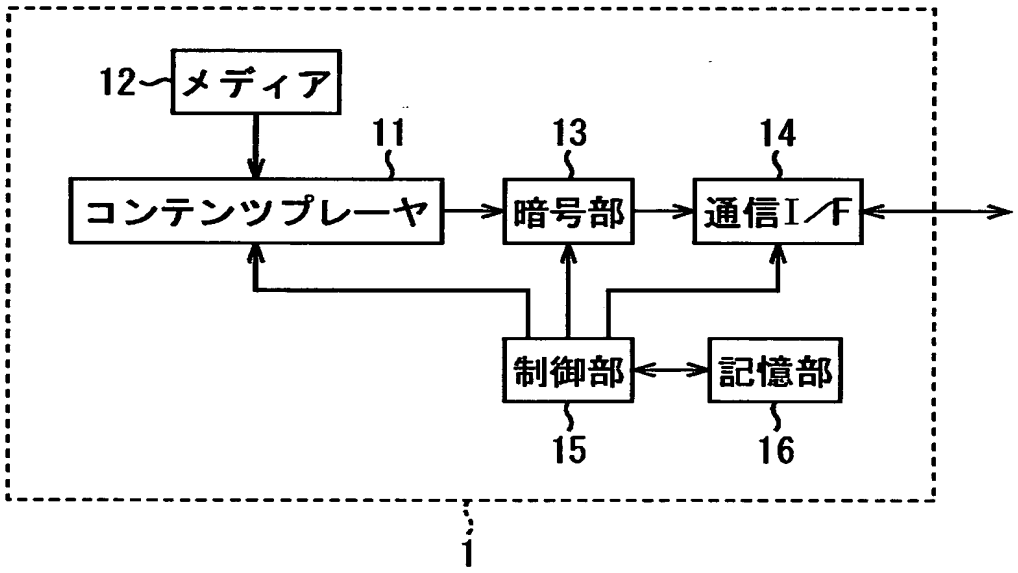
１　ソース，　２－１乃至２－４　シンク，　３－１，３－２　ブリッジ，１１　コンテンツプレーヤ，　１２　メディア，　１３　暗号部，　１４　通信I/F，　１５　制御部，　１６　記憶部，　２１　画像・音声出力部，　２２　復号部，　２３　通信I/F，　２４制御部，　２５　記憶部，　３１　通信I/F，　３２　復号部，　３３　暗号部，　３４　通信I/F，　３５　制御部，　３６　記憶部

【書類名】図面

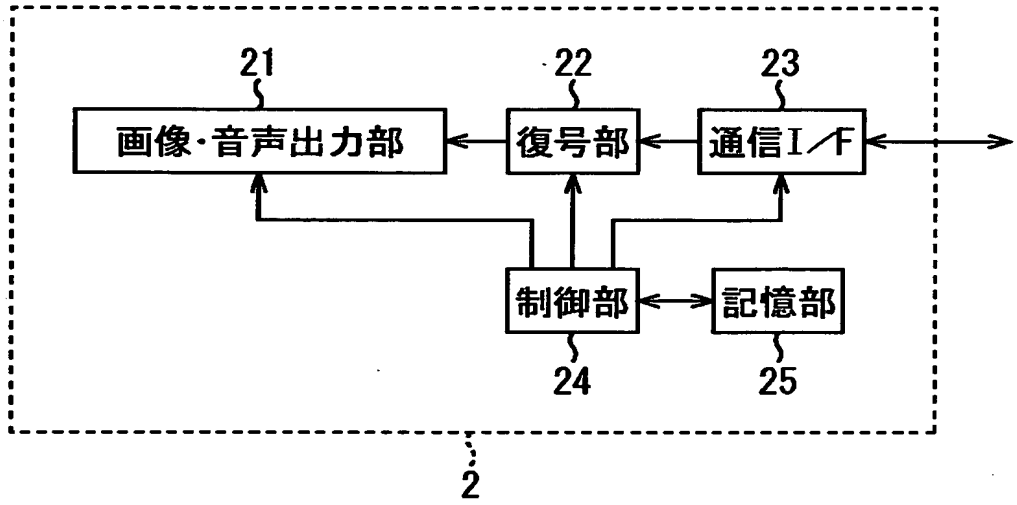
【図１】


1
ソース
4−1
3−1
4−2
3−2
4−3
ブリッジ
ブリッジ
シンク
シンク
シンク
シンク
2−1
2−2
2−3
2−4

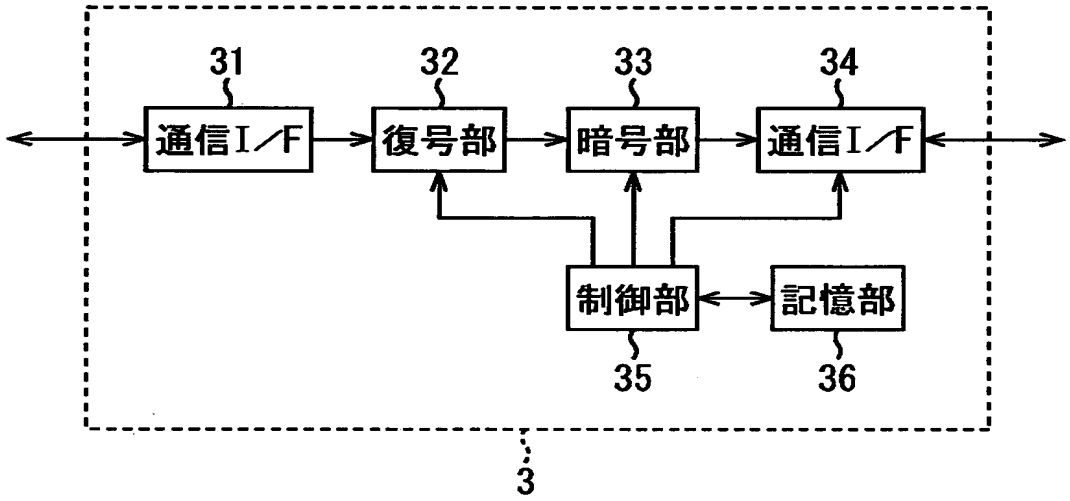
【図２】


12
メディア
11
13
14
コンテンツプレーヤ
暗号部
通信I／F
制御部
記憶部
15
16
1

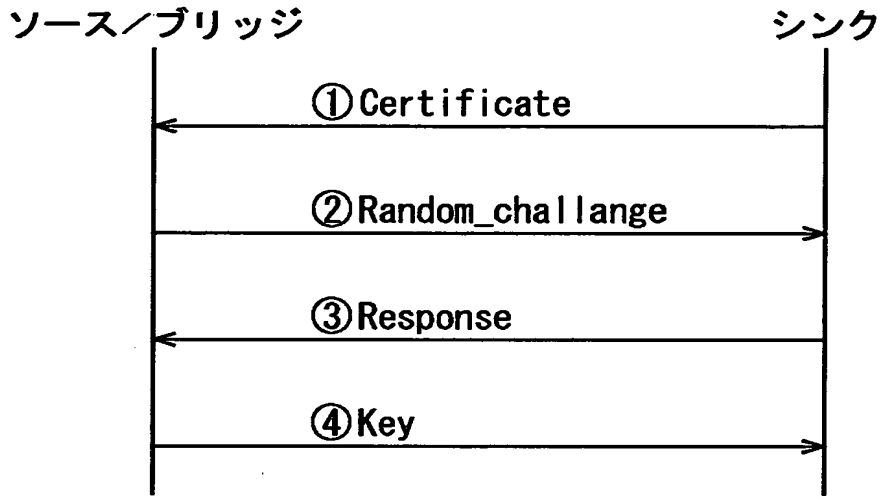
【図３】


21
22
23
画像･音声出力部
復号部
通信I／F
制御部
記憶部
24
25
2

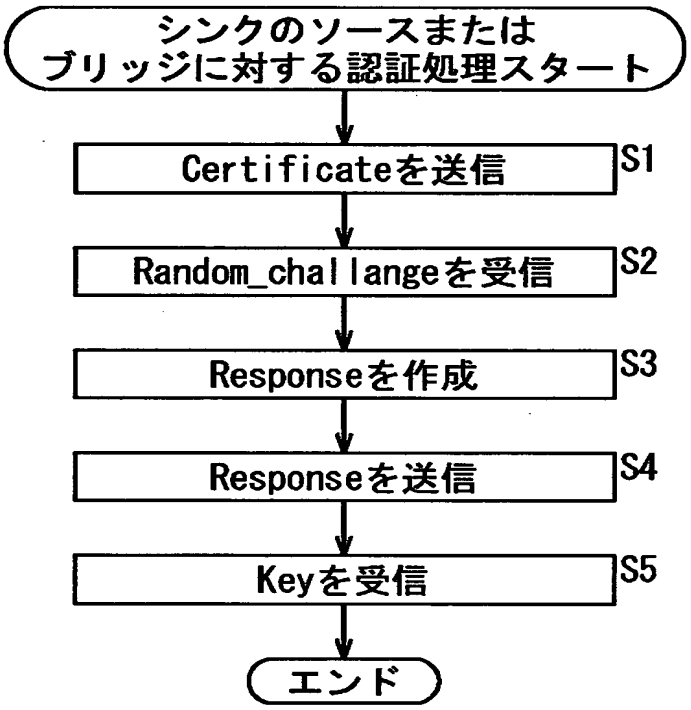
【図４】


31
32
33
34
通信I／F
復号部
暗号部
通信I／F
制御部
記憶部
35
36
3

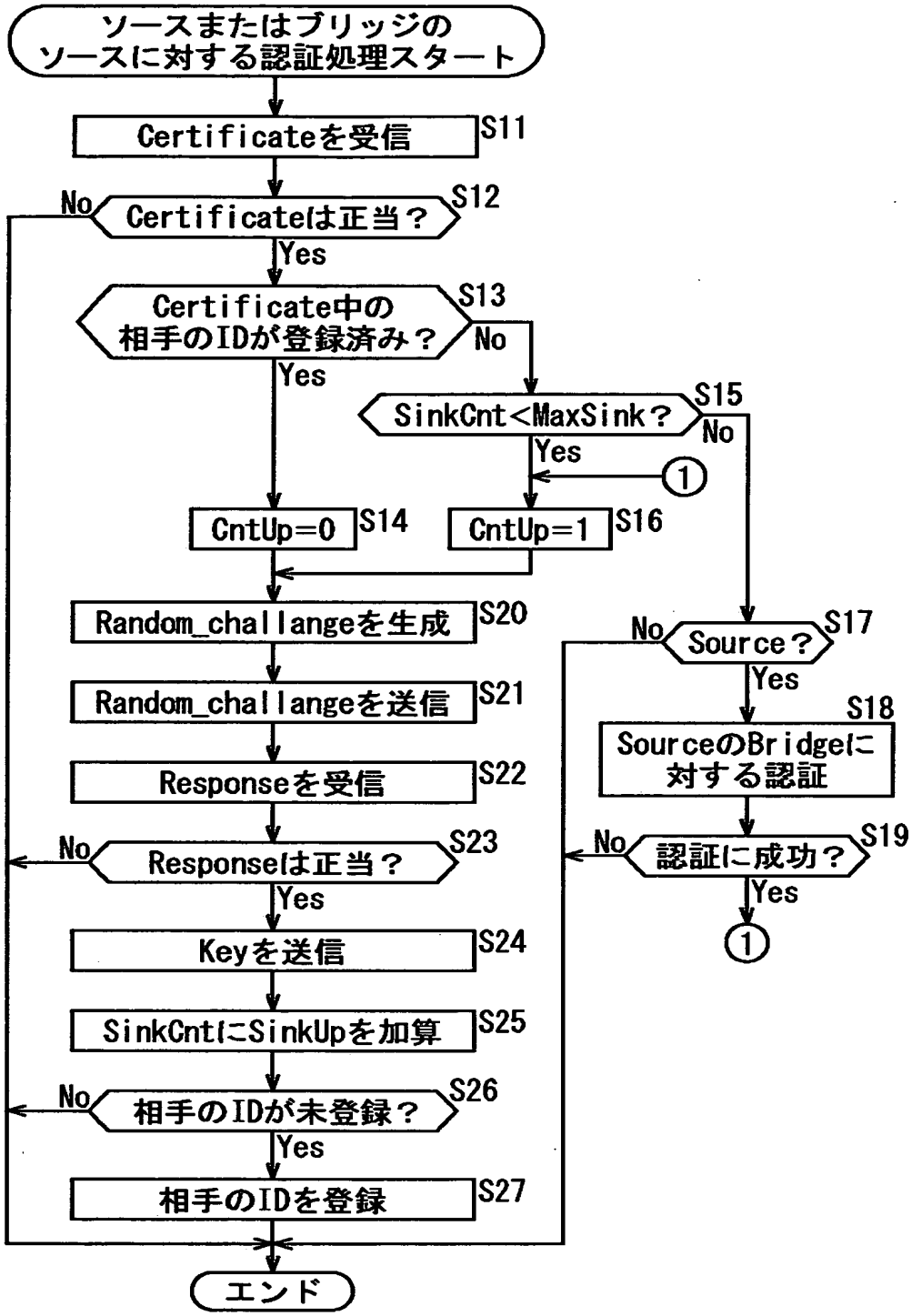
【図５】


ソース／ブリッジ
シンク
①Certificate
②Random_challange
③Response
④Key

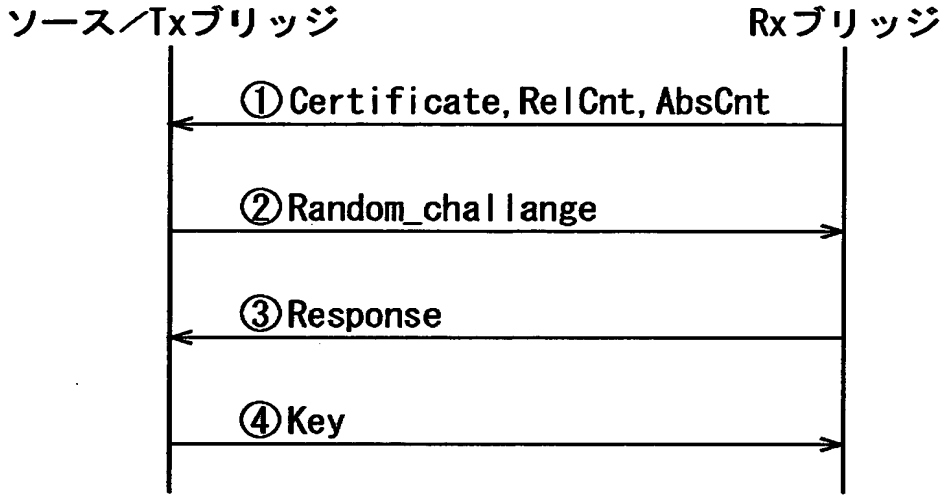
【図６】


シンクのソースまたは
ブリッジに対する認証処理スタート
Certificateを送信
S1
Random_challangeを受信
S2
Responseを作成
S3
Responseを送信
S4
Keyを受信
S5
エンド

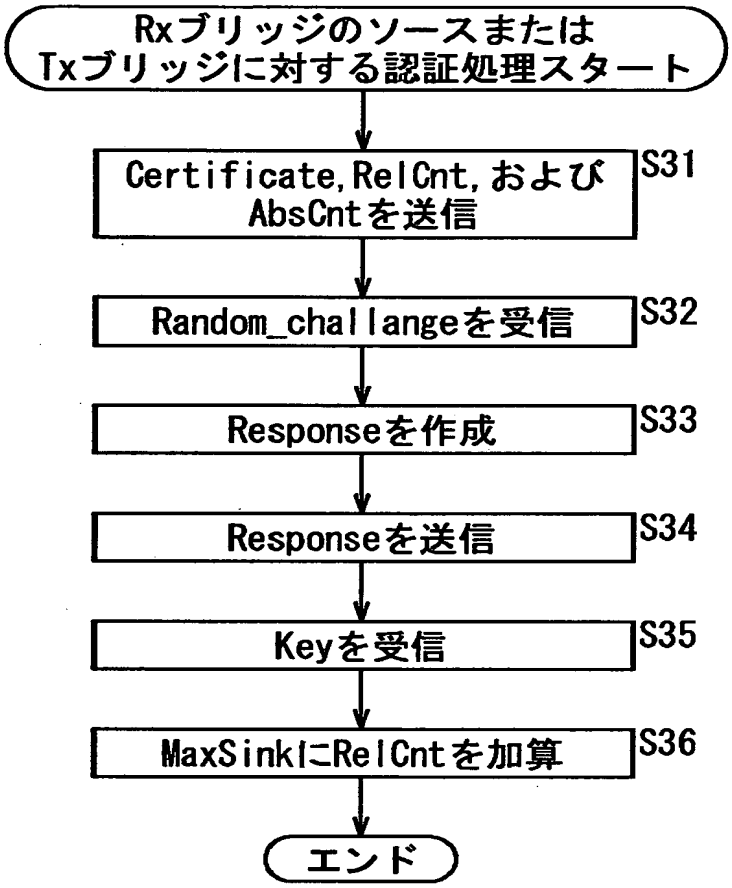
【図７】


ソースまたはブリッジの
ソースに対する認証処理スタート
Certificateを受信
S11
No
Certificateは正当？
S12
Yes
Certificate中の
相手のIDが登録済み？
S13
No
Yes
SinkCnt<MaxSink？
S15
No
Yes
①
CntUp=0
S14
CntUp=1
S16
Random_challangeを生成
S20
Random_challangeを送信
S21
Responseを受信
S22
No
Responseは正当？
S23
Yes
Keyを送信
S24
SinkCntにSinkUpを加算
S25
No
相手のIDが未登録？
S26
Yes
相手のIDを登録
S27
エンド
No
Source？
S17
Yes
SourceのBridgeに
対する認証
S18
No
認証に成功？
S19
Yes
①

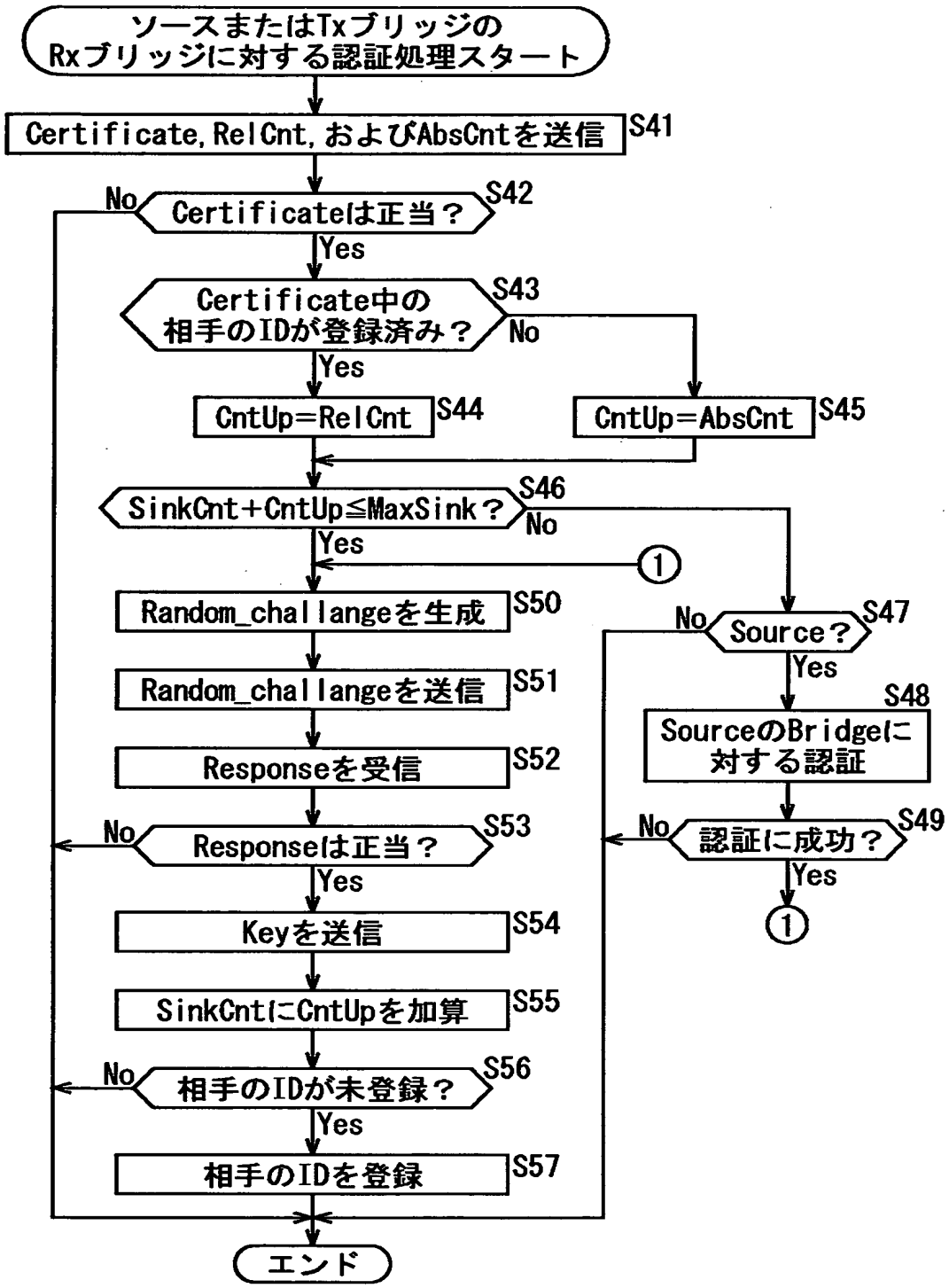
【図８】


ソース／Txブリッジ
Rxブリッジ
①Certificate,RelCnt,AbsCnt
②Random_challange
③Response
④Key

【図９】


Rxブリッジのソースまたは
Txブリッジに対する認証処理スタート
Certificate,RelCnt,および
AbsCntを送信
S31
Random_challangeを受信
S32
Responseを作成
S33
Responseを送信
S34
Keyを受信
S35
MaxSinkにRelCntを加算
S36
エンド

【図１０】


ソースまたはTxブリッジの
Rxブリッジに対する認証処理スタート
Certificate,RelCnt,およびAbsCntを送信
S41
No
Certificateは正当？
S42
Yes
Certificate中の
相手のIDが登録済み？
S43
No
Yes
CntUp=RelCnt
S44
CntUp=AbsCnt
S45
SinkCnt+CntUp≦MaxSink？
S46
No
Yes
①
Random_challangeを生成
S50
Random_challangeを送信
S51
Responseを受信
S52
No
Responseは正当？
S53
Yes
Keyを送信
S54
SinkCntにCntUpを加算
S55
No
相手のIDが未登録？
S56
Yes
相手のIDを登録
S57
エンド
No
Source？
S47
Yes
SourceのBridgeに
対する認証
S48
No
認証に成功？
S49
Yes
①

【書類名】　　要約書

【要約】

【課題】　コンテンツの利用を制限することができるようにする。

【解決手段】　ソース１は、シンク２－１よりコンテンツの送信要求を受けた場合、認証処理を行う。そして、認証に成功した場合、ソース１は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク２－１に送信する。シンク２－１は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことにより、コンテンツを受信することができる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－２１１７８７
受付番号	５００００８８０９０７
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１２年　７月１７日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100082131
【住所又は居所】	東京都新宿区西新宿７丁目５番８号　ＧＯＷＡ西新宿ビル６Ｆ　稲本国際特許事務所
【氏名又は名称】	稲本　義雄

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社